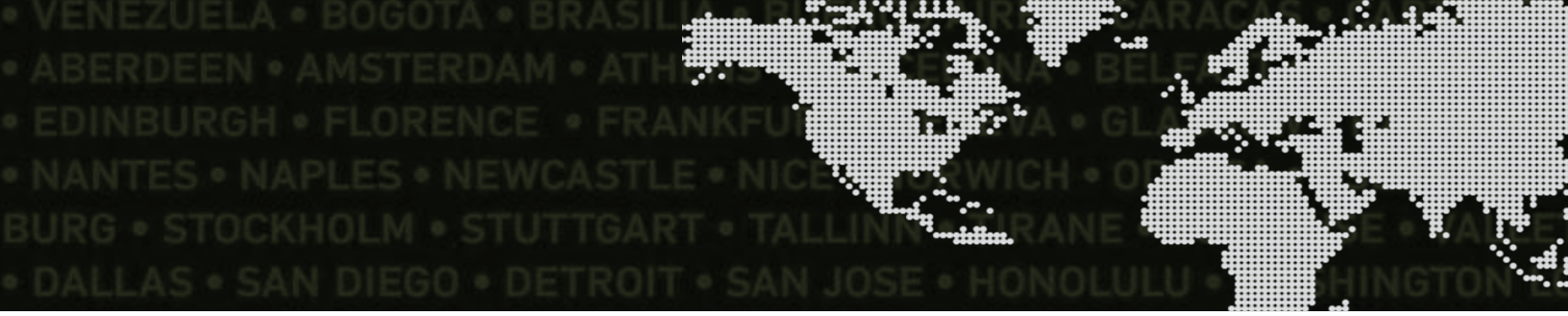

"A Failed State of Security" Part II

An Analysis of Causality and Cybercrime Victim Blaming

Chris Mark, *CISSP, CIPP*

www.MarkConsultingGroup.com

www.GlobalRiskInfo.com

chris@markconsultinggroup.com

Table of Contents

Forward 3

Introduction 3

A Brief History of Victim Blaming and Victimology 5

Understanding Cause and Causality 7

- The Philosophical View of Causality 8
  - A Brief History of Logic 8
  - Understanding Logical Fallacies 9
  - Philosophical definitions of Cause 9
- Fallacies of Correlation and Causation 10
  - Cum hoc, ergo propter hoc 11
  - Post hoc, ergo propter hoc 11
- Contributing, Enabling, and Proximate Factors 12
- Legal Context of Cause 12
  - Criminal Law 13
  - Civil Law 13

Victim Blaming Example 16

- A Philosophical Perspective 16
- A Legal View: “Shame…for Security Breach” 16
- Duty, Due Care and Negligence 16
- Who is really to blame? 18

Multidimensional Failures (industry, system, law enforcement) 18

Conclusion 21

About the Author 22

Disclaimer 22

Endnotes 23

Forward

This paper is part II of the series titled "Failed State of Security" which discusses failings within the information security industry. The first part is titled: *Failed State of Security"; A Rational Analysis of Deterrence Theory & Its Effect on Cybercrime*." The paper can be found on the Institute for Defense and Government Analysis (IDGA) website at: http://www.idga.org/intelligence/white-papers/a-rational-analysis-of-deterrence-theory-and-the-e/

Introduction

Some may argue that it is human nature to occasionally take joy in the misfortune of others and believe that some people who experience misfortune *"…got what they deserved"* or that they *"… had it coming".* Likely every reader (and this author) has, at one point or another, taken pleasure in another's misfortunate or possibly believed that the victim was wholly or partially responsible for their own victimization. While arguably a less attractive part of human nature, it would be disingenuous to ignore the fact that it may be emotionally appealing to believe that some victims of misfortune simply received their comeuppance. There is a German word that describes this very feeling. *Schadenfreude* is defined as "…taking pleasure from other's misfortune."[i] While taking pleasure or blaming a human victim of a crime is not uncommon, when the victim is a "faceless" corporation, it is perhaps easier and more appealing point the accusing finger at the victim and blame them for their own misfortune.

In the wake of the most recently publicized data breach, the perpetually circling media sharks and legal wolves have found a new opportunity to attack the victim of a crime. Reports indicate that within 1 day of the publication of the breach, at least one lawsuit had already been filed and by January 6th, 2014, least 40 lawsuits had already been filed in a variety of states.[ii] Additionally, numerous self-proclaimed "experts" have been quick to take advantage of media opportunities to opine on the causes of the breach and to point a proverbial finger at the victim whom they view as the sole responsible party. Regardless of the particular circumstances, and often without any knowledge of the situation, victim blaming by the media, the government, and plaintiffs is now a standard practice in the aftermath of a data breach.

On December 26th, 2013, while standing in front of a major retailer that had recently been the victim of a data breach, New Jersey Democratic Senator Bob Menendez stated publicly that he wanted to ensure retailers are not "putting their customers ahead of profits." He then stated*:*

> *"If in fact you have a company, …, that is not making the investment in their security process to* ***ensure that what happened to [victim company]doesn't happen****,"* he said on Thursday morning*, "then you have to question why a company would not do that."* (Emphasis added).

Capitalizing on the media frenzy initiated by the breach, on January 4th, 2014 CNN, a major news organization, posted an article titled: *"Shame on [company name1], [company name 2]for security breach".* Both of these statements indicate a continuing trend of ascribing the blame to the victim of a

crime while either ignoring the actual causes of the crime or the responsibility of the offender. In 1973, one of the forefathers of "victimology," Dr. Karmen stated in his groundbreaking book Crime Victims:

> *"Car stealing seems to be the only crime for which there is an organized victim-blaming lobby, a particular situation that developed long ago. Comprised of representatives of auto-makers, insurance companies, and law enforcement agencies, this lobby has castigated motorist carelessness since the dawn of the automobile age."*[iii]

As can be seen by the actions of at least two US Senators, a major news organization, and the numerous legal cases filed in the wake of the most recent breach, and extending back to at least 2005, the data security industry has the dubious distinction of having developed its own *'organized victim blaming lobby'*.

Conspicuously absent in the references to the most recent data breaches is mention of the criminal, or the efforts being undertaken to improve the legal landscape or law enforcement efforts to deter such actions. Instead of taking steps to improve crime deterrence, the victim is blamed for the shortcomings of the industry and law enforcement efforts. We have reached a point of requiring companies to engage in victim prevention instead of expecting "crime prevention".

The concept of blaming the victim of a crime, also called "victim facilitation," "victim precipitation," and "victim shaming", is certainly not a new concept. While it may be intuitive for people to develop conclusions based upon what they perceive as the causes of a particular event, too often these conclusions are, at best, premature, or, at worst, simply wrong. The unfortunate result, however, is that even when the victim is exonerated, they have already been branded with a scarlet letter regarding their role in the crime. In his article "The Ideology of Victim Precipitation," Douglas Timmer sums up the concept of victim blaming succinctly when he says *"…Wherever victim precipitation is offered as an explanation, it serves to place responsibility on the victim: you cause, or help to cause, your own victimization; you deserve what you get."* Adding to this Timmer states that:

> *"..Victim Precipitation Ideology blames neither the structure of society nor the individual offender for the crime. Instead it blames the victim who precipitates the crime.. This serves to excuse and legitimate a failing criminal justice system and absolve the criminal of responsibility."* [iv]

A quick internet search will provide ample evidence that blaming the victims of cybercrimes is rampant, accepted, and results in an increasingly complex and arduous regulatory environment in which to work. To date, nearly 4 dozen states have data breach notification laws while few have taken steps to prevent cybercrime or punish those who commit such offenses.

This paper will review the concepts of victim precipitation and argue that, while it may be appear palatable to place the blame at the feet of a large, faceless corporation for being victimized than it is to blame an individual victim of a violent crime, the blame in both cases is misdirected.

A Brief History of Victim Blaming and Victimology

Without a doubt victim blaming is as old as crime itself. The term 'victim' can be traced to 1,500 CE and was used to describe a *"living creature killed and offered as a sacrifice to a deity or supernatural being."*[v] Today, the term victim has evolved to refer to those who suffer injuries, losses, or hardships for any reason. People (natural and legal) can be victims of accidents, natural disasters, diseases, or social problems such as crime. **Crime victims are those who are harmed by illegal acts.**[vi] (Emphasis added)

Victimology, a subset of criminology, was developed in the middle of the 20th Century by attorney Benjamin Mendelsohn. Victimology was focused upon understanding the victim-offender relationship and the harm suffered by the victim as a result of the offense. To understand the relationship Mendelsohn developed a questionnaire and a topology that he argued identified "degrees" of victim culpability. With this topology "victim blaming" was legitimized. A more contemporary sociologist has commented that:

> "*…by raising questions about the victim proneness, vulnerability, and accountability, Mendelsohn put forward a more complete but also more controversial explanation about why laws are broken and people are hurt."*[vii]

The concept of "victim precipitation" originated with Wolfgang in his 1958 study Victim precipitated criminal homicide, which evaluated homicides in Philadelphia. The term was applied to an individual who was a *"direct positive precipitator in a crime"*[viii]. One example of the concept is where a victim started a fight and was subsequently killed by the party with whom they started the fight. In this scenario, it is clear that the victim had some degree of culpability in the resulting action. Unfortunately, this concept of victim precipitation has been expanded to include any action or inaction by the victim to include negligence, carelessness, and even vulnerability.

One of the most common and disturbing examples of victim precipitation can be found in the blaming of sexual assault victims. Although sexual assault has been blamed on victims since well before the term *victim precipitation* was coined, the concept served to legitimize the argument in the minds of many criminologists. A 1971 study that labeled 19% of rape victims in Philadelphia as "victim precipitated" stated: *"Thus the offender may see the victim's behavior as being contrary to the expectations about appropriate female behavior as well as conflicting with the whole image of women's propriety."* Defense attorneys argued that the victim provoked the attack by dressing "provocatively" or acting with "impropriety". This strategy was so frequently used in defending rapists that the strategy of victim blaming in sexual assault cases was given a name – the "mini-skirt defense". As late as 2013 the justice system was blaming victims of sexual assault. In one particularly disturbing case, a Montana teacher, who was convicted of raping a 14 year old student, was sentenced to only 1 month in prison. In the sentencing, the judge indicated that the young victim "shared responsibility" for her rape because she had some control over the situation.[ix]

While the legal system has, for the most part, moved away from victim blaming in sexual assault cases, a quick read through the papers or an internet search will reveal that there are those in society who still point the finger at the victim in sexual assault cases.

In 1979, Dr. Ezzat Fattah, in referring to victims roles in crimes wrote:

> *"Referring to the victim's negligence or carelessness and pointing out the victim's reckless, heedless, or imprudent behavior are the victimologists way of emphasizing the importance of situational variables and stressing the close link between crimes and environmental opportunities."*[x]

R. Block, added to his own opinion in 1980, when he said:

> *"The study of crime victims is primarily the study of the failure of crime prevention by citizenry and by the police and secondarily the study of the active participation and precipitation of criminal events by their victims."*[xi]

Because 'victim precipitation' is conceptually easy to understand, and possibly because it appeals to the schadenfreude in human nature, the concept of victim precipitation has expanded to include property crimes, financial crimes, and other forms of 'non-violent' crime. As can be seen in the article title in the introduction, the idea that the victim "caused the crime", "had it coming" or received "their just desserts" for their behavior is often intellectually and emotionally appealing.

Two theories have been put forth regarding the attribution of responsibly to victims. The first, known as the Just World Theory posits that the world is a largely fair and safe place to live and those who are victimized are so treated as a response to their own action or inaction.[xii] The second theory is known as the Defensive Attribution Hypothesis which is motivated by those who believe in an internal locus of control. In short, by believing that the victim was not responsible for their own victimization, a person would need to accept that they, too, could be victimized. For many, this is an uncomfortable concept to accept.

It should be noted that prominent researchers have been critical of victim blaming strategies in general. Timmer and Norman state that victim-blaming: *"…ignores and denies the role of the criminogenic social structure."* They further state: *"Explanations which blame the victim, as well as prevention strategies that focus on victim responsibility, are of little utility in controlling or preventing crime."* Finally, their statement is more direct and certainly more applicable to the current state of cybercrime when they say: *"The idea that these strategies are oriented toward victimization prevention, not crime prevention, is borne out by their inability to control or prevent crime."*[xiii]

In cybercrime attacks it is possible that the company alone is not the sole victim of the crime. If a customer's personal data is stolen and fraudulently used, then they too may be a victim. The concept of due care and other aspects of this type of scenario are outlined later in this paper.

A review of the current state of data **breach notification** laws and comments by government and law enforcement officials are equally instructive. Between 2002 and 2013, nearly 4 dozen different states have adopted 'data breach notification laws' which require a company that is victimized by a cybercriminal to disclose the breach to those customers who may be affected. During this same time, few, if any, laws have been passed that increase the penalties for perpetrating those criminal acts. Even the language used by the Honorable Mr. Menendez speaks of victimization prevention as opposed to crime prevention when he said:

> *"If in fact you have a company, whether it be [company name] or any other, that is not making the investment in their security process to* ***ensure that what happened to [company] doesn't happen****,"* he said on Thursday morning*, "then you have to question why a company would not do that."* (Emphasis added).

There is an old adage that *"opportunity makes the thief*." This has been formalized in opportunity theories of crime prevention such as Situational Crime Prevention (SCP) and Routine Activities Theory (RAT). Opportunity is defined by Miriam Webster's dictionary as: *"…a favorable juncture of circumstances"*[xiv]. Routine Activities Theory posits that multiple variables impact crime however, believe that opportunity represents the variable with the greatest impact. Some criminologists have argued that opportunity alone does, in fact, make the thief. '

> *"The most significant, and universal cause is, however, opportunity. If there were no opportunities there would be no crimes; the same cannot be said for any of the other contributory causes. In so far as opportunity creates criminality by rewarding those with low motivation with success in easily chosen and completed crime, it thus comprises a root cause - as one recent paper puts it, 'Opportunity makes the thief'"*[xv]

While this paper is not intended to be a discourse on criminology, even the expression "opportunity makes the thief" places blame of a crime on the shoulders of the victim by proposing that without such opportunity the criminal would not be motivated to commit the crime. It is suggested that it is more appropriate to state that *"Opportunity makes the thief ('s) job easier"*.

Understanding Cause and Causality

The simple term "cause" can be deceptively complex to understand and apply. The application becomes much more difficult when applied to social issues and events where ambiguity, subjectivity, and moral and ethical aspects must be considered. While the concept of cause and causality has been studied and debated by philosophers for millennia a commonly accepted definition is still not found. It was Virgil who, in Georgics 2 in 490 said*: "Felix qui potuit rerum cognoscere causas"* or "*blessed accomplishment theirs, who can track the causes of things*".[xvi] The difficulty of defining the concept of "cause" is familiar to those with an interest in philosophy or science. Without becoming a primer on the intricacies of the debate, suffice it to say that cause, like security, is necessarily contextual in nature. Within the context

of Victimology, it is important to understand the distinction between identifying what a person emotionally or philosophically believes is a 'cause' of an event that impacts a victim and the philosophical and legal concepts of 'cause' as they applies to a crime.

The Philosophical View of Causality

As discussed in the introduction to this paper, people often ascribe blame based upon their internal logical calculus or emotional belief that the victim may have played a role in their own misfortune. For this reason, it is important to understand the philosophical underpinnings of reasoning and how they apply to determining 'cause'. As important is the understanding of errors in logics. Within logic, errors in either reasoning or structure are known as fallacies. With an understanding of the common fallacies that pertain to identification of cause, it is easier to understand and identify the true, or actual cause of an event.

Logic, or reasoning, is described as *scientia scientiarum* or the *science of science* for the prominent and important role reasoning plays in the sciences[xvii]. While formal logic has been studied for at least two millennia, and informal logic for nearly one millennium, it is the theory of fallacies that provides the tools for critical thought. UNLV's Distinguished Professor of Philosophy; Emeritus Maurice Finnocchiaro stated that fallacies: *"may be interpreted as a more relevant contribution to the evaluation of reasoning"*[xviii]. Kirby and Goodpaster stated in 2007 that*: "Thinking logically and identifying reasoning fallacies in one's own and in other's thinking is the heart of critical thinking"*[xix]*.* The search for cause requires an understanding of logic as well as the common fallacies that relate to the concept.

A Brief History of Logic

In his seminal 1893 work *Logic; Inductive and Deductive*, William Minto stated that logic could be defined as a*: "…system of defense against error"* with the objective being the "*…organization of reason against confusion and falsehood".* While the evolution of Logic extends to Aristotle and his focus on dialectics it was in the 13th Century when Bacon articulated the concept of inductive logic that saw the creation to a separate, though related branch of study. In Sir Francis Bacon's *Opus Majus*, he stated*, "There are two ways of knowing, by Argument and by Experience. Argument concludes a question, but it does not make us feel certain, unless the truth be also found in experience".* Minto also posited that *logic "…shows the inquirer how to test and purge his conclusions, not how to reach them".*[xx] Applying logic, therefore, is necessary to understand whether a stated position is valid or not.

Deductive, or formal, logic is a type of reasoning in which two or more premises are offered and then a conclusion is derived that, by definition, must follow from the premises. The structure is known as a syllogism and is critical to evaluating the validity of the argument. If the premises of a formal argument are valid then the conclusion must, by rule, be valid[xxi]. Inductive or informal logic, by contrast, presents premises to support a conclusion but the conclusion is not guaranteed to follow from the premises[xxii].

Mr. Bennett stated, *"Arguments where the conclusion is merely based on probability, not necessity, are considered inductive arguments".*[xxiii] The Cambridge Dictionary of Philosophy defines inductive logic as:

"… most generally … the theory of the evaluation of ampliative inference".[xxiv] In short, in deductive logic, the conclusion of a valid deductive syllogism must be valid, whereas in inductive logic the conclusions are only likely to be valid. Inductive or informal reasoning then is the type of reasoning that people apply on a daily basis. As the validity of an inductive argument is based upon "ampliative inference" both errors in logic as well as errors in the structure of the argument can influence the inference that is taken from the presented evidence. For this reason it is critical to understand the fallacies that affect such forms of reasoning and particularly those that impact the identification of cause.

Understanding Logical Fallacies

As stated previously, the theory of fallacies can be interpreted as the evaluation of reasoning[xxv]. To quote the ubiquitous Wikipedia a fallacy is defined as *"…an argument that uses poor reasoning."*[xxvi] Fallacies then are either an error in the argument's structure or an error in the reasoning provided in the argument. The argument is the fundamental unit of reasoning[xxvii] and the structure and content of an argument impacts the truth or validity of the conclusions[xxviii]. For over 2 millennia philosophers have debated and studied the theory of fallacies and have attempted to define the various fallacies that affect reasoning. At the writing of this paper over three hundred informal fallacies have been identified[xxix]. As Minto stated: "*It is the existence of Fallacies that calls Logic into existence; as a practical science Logic is needed as a protection against Fallacies."*[xxx]

While the construct of logic contains hundreds of fallacies in four major groups, they can be grouped into the two general categories of informal and formal logical fallacies. In simple terms, formal fallacies have an error in structure of the argument.[xxxi] Informal fallacies, on the other hand, have correct structure but the content of the argument has errors.[xxxii] *"…an informal fallacy is a fallacy that isn't covered by some system of deductive or inductive logic"*. Formal and informal fallacies are present in both deductive and inductive forms of logic. Given that formal fallacies result only from the structure of an argument and not the content, they are, as Finocchiaro *said "…conceptually indistinguishable from the theory of validity, since, as the textbooks point out, a formal fallacy may be regarded as any (formally) invalid argument…"*.[xxxiii] This is not to suggest that formal fallacies are any less important to the evaluation or reasoning, rather simply to identify that they represent a different criteria of evaluation.

With a basic understanding of formal and informal logic, as well as formal and informal fallacies, it becomes easier to understand if and when a presented argument is fallacious. Causality is so critical to logic and daily life that philosophers have studied the concept for millennia and causality has numerous fallacies specific to the argument of causality.

Philosophical definitions of Cause

Numerous definitions of cause can be found throughout philosophy. In his Regularity View of Causation (RVC), the philosopher David Hume described Cause when he said:

> *"We may define a CAUSE to be ""An object precedent and contiguous to another, and where all the objects resembling the former are plac'd in like relations of precedency and contiguity to those objects, that resemble the latter""*[xxxiv]

While philosophical definitions of cause give some insight into the origins of our existing definitions and provide interesting fodder for debate, they are often not functionally useful or appropriate for viewing a social act such as an intentional criminal event. Philosophy aside, an effective working definition of cause that applies the various philosophical definitions is put forth by Julian Meltzof in his book *Critical Thinking about Research*, when he defined cause as:

> *"A **proximal antecedent** is an agent or agency **that initiates** a **sequence of events** that are necessary and sufficient in bringing about the observed effects."(Emphasis added)*

Using Meltzof's definition, it is apparent that an 'agent' or 'agency' must be the 'initiator' of the sequence of the events and be a 'proximal antecedent' to the sequence of events that brings about the effect in which we are currently interested: crime. Using this definition in the context of a data breach supports the position that if a person or persons initiated a sequence of events that exploited vulnerabilities which resulted in the compromise of systems or data, the person is therefore the *actual cause* of the compromise. The agent, in this case the person who initiated the sequence of events, is antecedent in that it preceded the effect (in this case the compromise of data) and it is proximal in that the initiating action is not too far removed from a temporal perspective as to raise doubts about the cause. In short, a direct line of cause and effect can be drawn between the initial action which set the sequence in motion and the effect that resulted.

It is important to note the two additional aspects of cause. The sequence of events initiated by the agent must be necessary and sufficient to bring about the effects. Consider a situation in which a person we will call Bill fires a gun that kills another person. Without using a definition such as that provided by Meltzof, it could be argued that any number of factors, including Bill, were the "cause" of the fatality. One could blame the gun, the bullet, the firing pin, or even the propellant that fired the projectile. Using the provided definition, it is clear that the proximal antecedent that initiated the chain of events is Bill, who pulled the trigger on the firearm which, in turn initiated the sequence of events (firing pin hits primer, primer ignites propellant, propellant burns creating pressure, pressure accelerates the bullet through the barrel etc) that resulted in the death of the other person. This is an important point to remember, as blame is often placed on the victim of cybercrime for not taking greater precautions to prevent the sequence of events from occurring when, in fact, it is the person initiating the sequence of evince that is the actual or primary cause.

Fallacies of Correlation and Causation

Correlation and causation are so frequently confused or intertwined that it merits discussion in this paper. Cause, as defined by Meltzoff and many other philosophers, requires that an initiating action be a 'proximal antecedent' to the effect. It is this temporal and structural relationship (ie. One event

precedes another) that provides fertile ground for those seeking to find cause to make fallacious arguments or reach incorrect conclusions.

As any college statistics student can attest, correlations between variables simply show whether, and to what degree, a relationship exists. The fact that there is a relationship (positive or negative) between the variables does not imply that one is the cause of the other. A positive correlation simply means that as one variable moves in one direction, the other(s) move in the same direction. A negative correlation simply means that as a variable moves in one direction the other(s) move in an opposite direction. Positive correlations are particularly relevant to the issue of assigning blame in data breaches as people can often mistake a correlation with causation. As an example, there is a demonstrated positive correlation between the incidence of snakebites and the weekly consumption of ice cream in the Southwestern United States.[xxxv] In areas where people eat more ice cream they also experience more snake bites. This, however, is due to the geographic location and warmer weather in which people tend to prefer ice cream and which also happens to be more habitable for snakes. The increased consumption of ice cream is unrelated to the increase in snake bites. This simply means that as X increases, so too does Y. In spite of the correlation, one cannot say that the former causes the latter to happen.[xxxvi] There is another observed correlation between chocolate consumption and the number of Nobel Prizes per capita.[xxxvii]

The provided are examples of spurious relationships. A spurious relationship is a relationship in which two events or variables have no direct causal connection, yet it may be wrongly inferred that they do, due to either coincidence or the presence of a certain third, unseen factor (referred to as a "confounding factor" or "lurking variable")[xxxviii]. If no coincidence is present then it is the third, or 'confounding variable' that implies causality. As stated previously, it is the warm weather in the Southwest that creates an environment in which more ice cream is consumed, people are more active, and snakes are more active. This results in a spurious relationship in which ice cream consumption and snakebites are positively correlated yet not causally related.

Cum hoc, ergo propter hoc

Com hoc, ergo propter hoc is a Latin phrase that describes a common error fallacy within the Questionable Cause (*non causa, pro causa*) informal logical category. It describes a situation, like that described between snakebites and ice cream, where people believe that *correlation implies causation*. Without further information or understanding it is possible that the correlation between two events is simply spurious and has no causal relationship. Understanding causation and correlation and what, if any, relationship exists between the two is important for those trying to ascribe blame for a crime.

Post hoc, ergo propter hoc

Another fallacy that is often made in the evaluation of cause is that of *post hoc, ergo propter hoc*. Translated roughly as "*after this, therefore because of this"* in Latin. It is the mistaken belief that one condition preceding another condition must necessarily cause the succeeding event.[xxxix] Fans of professional baseball can witness *post hoc, ergo propter hoc* when players are in a batting slump or are hitting well. Superstitious players will often adopt a ritual that they happened to have used **before**

hitting particularly well in the belief that somehow this ritual, by preceding the batting, **causes** the hitter to bat well. In reality it is nothing more than one event occurring before another event (a proximal antecedent event) and which has no causal effect. The previous examples can be considered spurious correlations or relationships in which two elements are correlated yet have no direct causal relationship.

Contributing, Enabling, and Proximate Factors

This paper's readers clearly understand that situations cannot arise in a vacuum and that even a victim's actions can increase the probability of an event occurring. For example, the simple act of walking to work will certainly increase the odds of a that person being hit by a car. The difficulty for many is understanding the difference between a contributing factor and one in which cause or blame for the event can be assigned.

Contributing or enabling factors can be defined as *"…a state or condition that allows something to happen that is not, by definition, the cause."* Contributing factors provide an easy target for those who wish to ascribe cause to the crime. People may confuse a condition which enables an action to occur as the actual cause of the event. Consider a person carrying a large sum of money who is subsequently robbed of said money. Without the money in their possession the robber could not have stolen the money from the victim. Regardless of the fact that the person was carrying the money, the presence of the money did not **cause** the robber to commit the crime. The robber that initiated the sequence of events that resulted in the effect (stolen money) **caused** the actual robbery. Did the presence of a large sum of money create a condition in which the victim was a more attractive target? Possibly. If the victim was walking down a dark alley in a questionable part of town some would argue that this also contributed to the event. The difficulty then is discerning when the victim is responsible for actions that may contribute and how to judge such actions or inactions.

In the event of a data breach initiated by a cybercriminal, it is possible that the actions of the company enabled the attack to occur or made the attack easier for the criminal, but the actions of the company were not the direct or actual cause of the incident. Put simply, certain conditions enable things to happen that probably would not happen otherwise. This, however, is not the cause of the event.

The ideas presented in this section are important to understand when evaluating a chain of events to find fault.

Legal Context of Cause

This section is not intended to be a discourse on law nor to provide legal advice, rather it is intended to provide a broad overview of the concepts of cause and causation as they are framed within a legal context. When discussing the legal definition of cause, one must consider the criminal as well as civil law, as there are differences between the two concepts. In most cybercrime situations, the companies who have been breached will face various accusations of negligence, among others. To help understand how the legal system views cause, it is important to have a working definition of several concepts. While this is interesting information to understand it is only relevant once a company that has experienced a data breach faces either criminal charges or civil complaints. Without exception, by the

time the court system has run its course, the victims have been tried and convicted in the court of public opinion.

Criminal Law

From a criminal standpoint it is difficult to lay blame at the feet of the victim unless their actions were, in fact, intentional (someone intentionally left their keys in their car and asked someone to steal said car) or rose to the level of criminal negligence. Consider a situation in which a parent leaves a loaded firearm unsecured in their home and a young child living in their home finds the firearm and shoots their sibling. This is a situation in which the courts may find that the parents' actions raised to the level of criminal negligence as it should be understood that young children do not understand the effects of firearms and parents should recognize the risk and take appropriate actions to prevent discharge of the firearm. Courts are unanimous that unless an action is the sole proximate cause of the resulting harm, the victim's conduct is irrelevant to the case.

Now consider the following example with two outcomes. In the first situation a member of the Sharks (yes, from a Westside Story) enters an apartment with a Jet. The Shark, simply by virtue of wearing his "Sharks are better than Jets" t-shirt is attacked by the Jet and injured. Certainly, the Shark, by wearing the shirt announced that he was a Shark. This, however, does not make him responsible for the resulting crime committed against him. Now consider the same two members of the Sharks and Jets. The Shark walks into an apartment and sees a Jet wearing a shirt that says "Jets Rule; Sharks Drool". Angry at such an insult, the Shark pulls a knife to attack the Jet. The Jet, then pulls his own knife and injures the Shark. In this situation, it is the Sharks' own actions that initiated the sequence of events that resulted in the injury.

From a criminal perspective, it is extremely difficult to point an accusatory finger at a cybercrime victim. Nothing more on this subject needs to be said.

Civil Law

Many personal injury lawsuits, and most of those filed against companies who experience a data breach, are based upon the theory of negligence. Negligence is typically claimed in situations where it is believed the company that was breached did not "*do enough to protect consumer data*". Below are some relevant definitions and concepts that should be considered when attempting to ascribe blame to the victim of a data breach.

Negligence- The concept of negligence is the basis upon which almost all legal cases rely when attempting to ascribe blame to a company that was breached. For this reason, it is of paramount importance to understand the definition of negligence and the basis under which negligence is considered. Legal Dictionary.com defines Negligence as:

> *"Conduct that falls below the standards of behavior established by law for the protection of others against unreasonable risk of harm. A person has acted negligently if he or she has departed from the conduct expected of a* ***reasonably prudent person*** *acting under similar circumstances."*[xl]

This is an important concept as the litmus test rests on what a 'reasonably prudent person' would do in similar circumstances.

Duty – Another important concept related to data compromises is that of duty. A primary question that must be asked is *"did the company have a duty to protect the customer's data*?" Legal Dictionary.com defines duty as:

> "*n. 1) a legal obligation, the breach of which can result in liability. In a lawsuit a plaintiff must claim and prove that there was a duty by defendant to plaintiff. This can be a duty of care in a negligence case or a duty to perform in a contract case."* There is an interesting point to duty which protects a victim. In Hennessey v. Pyne the 'no duty' rule was interpreted to guard against "*…penalizing the victim in a situation ni which the victim might have acted stupidly or reprehensibly but did not violate legal duty."*[xli]

A particularly relevant situation arises when a person does not lock their house in a high crime neighborhood and their house is subsequently burglarized. There is no duty for a person to lock their house. The fact that the plaintiff did not lock their house does not diminish their ability for recovery against a burglar.

Due Care - Yet another concept that raises its head in data breach lawsuits involves that of due care. Legal Dictionary.com defines due care as

> *"n. the conduct that a reasonable man or woman will exercise in a particular situation, in looking out for the safety of others. If one uses due care then an injured party cannot prove negligence. This is one of those nebulous standards by which negligence is tested. Each juror has to determine what a "reasonable" man or woman would do."*

The concept of due care is particularly important in cybercrime breaches. Consider a situation in which the company did not encrypt data traversing a private, internal network and a cyberthief was able to capture sensitive data (ie. Credit card data). There is no law, regulation or industry mandate that requires encryption on a private network. In this instance, it is difficult to envision how a 'reasonable person' would believe that the company should have encrypted traffic on a private network.

Reasonable Person- The reasonableness standard described previously rests on the concept of a hypothetical person known as a 'reasonable person'. Legal Dictionary.com defines Reasonable Person as: "*… a hypothetical person in society who exercises average care, skill, and judgment in conduct and who serves as a comparative standard for determining liability."* In short, a company's obligation to act, if not dictated by law, regulation, or standard is that of how a 'reasonable person' would act in a similar situation.

Cause in Fact – This is an important point when attempting to view cause in the context of civil law. Cause in fact is a concept that requires that the defendant's negligent conduct (see below) was the **actual cause** of the plaintiff's injuries. This is also known as the "but-for" test. "But for" the defendant's

negligence, the plaintiff would not have been injured. Consider a situation in which a company knowingly ignores an icy sidewalk outside of their building on which people had already slipped and been hurt. An innocent mail carrier, during the course of his or her daily route, slips on the sidewalk and is injured. The mail carrier could potentially claim that the defendant's negligent conduct (Ie. Not clearing the ice) was the actual cause of the injuries. The argument would state that "but for" the negligence of not clearing the ice, the plaintiff would not have been injured. This point is particularly relevant in companies that have been breached and their own clients' personal data exposed. Those who had credit card, bank account, or other protected information may claim that "but for" the negligent conduct of the company who was breached, the customers of the company would not have been injured.

Proximate Cause – Finally, proximate cause relates to the 'foreseeability' of the injury and indicates that a party may be **partly responsible for the crime**. The proximate cause of an injury is the act or omission of an act without which the harm would not have occurred. This is a concept in the law of torts and involves the question of whether a defendant's conduct is so significant as to make him or her liable (or partly liable) for a resulting injury.[xlii]

With a basic introduction to some important legal definitions, it is possible to now further dissect some of the accusations against companies that are breached. First, it is important to understand that if a company is determined to have been 'hacked' or 'breached' by a third party and personally identifiable information (PII) or other regulated consumer data is subsequently exposed then they are likely the victim of a crime. The use of the phrase 'likely' is intentional because the courts will need to decide the guilt or innocence of the offending party.

Regardless, if a company's data is accessed or exposed by an unauthorized party then it is the unauthorized person who is the instigator of the event and the company's role is relegated to being a 'proximal cause' if it is determined that their actions or inactions were partly responsible. This will likely lead to claims of 'negligence' on the part of the victim, as it will be claimed that the company did not exercise "due care" in the protection of consumer data. This, again, is judged upon the "reasonableness" standard. First, it is necessary to establish that the company had a duty to those whose data was exposed. In the US, the Federal government, as well as most states, has laws which establish a duty of protection for PII, PHI and other types of sensitive consumer data.

With duty established, the plaintiff will assert that the victim did not exercise 'due care' in the protection of data. This is judged on the 'reasonableness' standard in which the victim's actions or inactions will be evaluated against the actions of a person with similar experience acting in a similar situation. This is a very important point to understand because many are quick to lay blame at the feet of the victim before any information is released and simply jump to conclusions about liability and blame.

Victim Blaming Example

In the introduction to this paper, the article titled "Shame on [Company Name] and [Company Name] for Security Breach" was referenced. This article is instructive and demonstrates a number of flaws in the assessment of the situation. A few of the more relevant points are below.

A Philosophical Perspective

As discussed previously cause can be defined as: *"A **proximal antecedent** agent or agency **that initiates** a **sequence of events** that are necessary and sufficient in bringing about the observed effects."* Given that the author of the "Shame" article acknowledges in each situation that the 'cause' of the breach was the event initiated by a "proximal antecedent agent", it is difficult to understand how he can point the finger solely at the victims. In the article, it seems as if the author is saying that the companies were responsible for their being victimized in spite of the fact that their actions did not initiate the sequence of events that resulted in said breach. Whether they are legally responsible (wholly or in part) is to the courts to decide.

A Legal View: "Shame…for Security Breach"

The title alone speaks volumes. When combined with the acknowledgement that each company was indeed 'hacked' by a third party, it appears as if the author is ignoring the culpability of the offending party and placing the blame squarely at the feet of the victims. As stated in the article: *"These are just the latest in a long list of tech companies that **fail to provide adequate protection of their users' personal data**." (Emphasis added)* The author does seem to delve into the legal side of the argument when he references the failure to *"…provide adequate protection of ….personal data."* Is this position accurate? Let us look further.

Duty, Due Care and Negligence

The author states with confidence that companies that offer free services have an obligation to protect data that is not classified as 'protected'. In the article he asked*: "Do companies that offer free services have an **obligation** to protect our **communications? Yes, absolutely."*** (Emphasis added). As discussed previously, there may be a duty to protect personal information, if it is classified as Personally Identifiable Information (PII), Protected Health Information (PHI) or another type of regulated data. Certainly with regard to PII, PHI, and other 'regulated' data, companies have a duty under various data protection and data breach notification laws to take steps to protect data. The assertion that companies that "…offer free services…" have an obligation to protect unregulated data that rises to the level of a duty to protect internet chats is debatable, at best. While it may be frustrating to have your personal communications exposed or your phone number published online, it likely does not rise to a legally actionable level.

When describing the second company in the article, the author stated: *"Didn't [company name] think the 27 million people who "liked" them on Facebook and the more than 3 million people who follow them on Twitter deserve to be protected from potentially malicious posts?"* The author now takes the company to task, not for having client's protected or personal information compromised but rather for

having a hacker post something on a blog that can be read and may be considered objectionable. What is a *"…potentially malicious post"?* Why would a user expect a company to expend valuable resources to prevent someone from simply posting an offensive comment? If a hacker did post an offensive comment, the crime that has been committed is against the company that was hacked and not the people who read the post. The author appears to lose perspective on this point. What is particularly troubling about this reference is that the author does not indicate any first-hand knowledge of the attack and simply makes a very loose correlation to the attack by asking: *"It must have been an extremely sophisticated hack, right?"*

The author then opines on the cause of the breach and answers his own question by saying: *"Unfortunately, the answer is no. The Syrian Electronic Army is **famous for using** phishing, a simple tool that persuades users to disclose their user names and passwords through cleverly worded e-mails." (Emphasis added.)* Again, there is no first-hand knowledge but this does not seem to dissuade the writer. He continues from a perspective of prior knowledge of how this particular group has acted in the past. The author then goes on to deride the victim for not taking appropriate precautions to protect its users from a *"… potentially malicious post"* caused by the spear phishing that the author does not acknowledge was the reason for the breach.

In the first case the only information disclosed was "usernames" and "phone numbers". While in certain instances (for example, a person who was using a private account to access a bank account or pornography and wished to remain anonymous) it could be argued that usernames and phone numbers could constitute Personally Identifiable Information (PII). Given that the company referenced was a social media company and that phone numbers are available in directors and a variety of other media, it is difficult to understand how this rises to the level of imposing a "duty" on the company to protect phone numbers.

The second case referenced in the article applies to a company that had, according to the author, a "potentially malicious post" posted to the blog which read: *"Hacked by Syrian Electronic Army ... Stop Spying!"* Was the **act** "malicious"? Arguably the poster acted with malice against the victim, but it is difficult to envision that a post imploring someone (the NSA?) to "…stop spying" is a malicious act against the readers of the blog. Did the Syrian Electronic Army gain unauthorized access to the service? Most likely they did. Did the victim have a duty to protect its users from such a "malicious" post? That is unlikely unless their privacy or other policy claims that they would protect their users from such actions. Consider the following example. A couple and their two young children are eating at a restaurant. A person runs into the restaurant and begins screaming to the patrons that the US should "stop spying." Is the restaurant responsible for not taking greater precautions to "protect its users from malicious yelling?" It is highly unlikely that the restaurant is responsible for such an action.

The last question is whether the company was indeed "negligent" by not exercising "due care"? The debate over the negligence is moot if there was not duty to protect against the claimed acts. For the sake of argument we will ignore the duty question and focus solely on the concept of negligence. Negligence requires that a person, or in this case a company, not exercise 'due care' in the protection of

data which it has 'duty' to protect. According to the story, and subsequent research, "security researchers" identified a vulnerability in the victim's code and contacted the company with an offer that they would be *"glad to help [company name] out".* There is no other context to this offer. When the company did not take up the magnanimous offer from the researchers, the researchers then publicly disclosed the vulnerability. According to the story, the victim indicated that they had *"…recently added additional counter-measures and continue to make improvements to combat spam and abuse."*[xliii] If one believes that the company had taken what they felt to be necessary steps to prevent the breach, then it is difficult to consider them negligent. If, as the author suggests, the negligence arises from the company not engaging the 'researchers' for their help, then it is easier to justify. It seems that the "researchers" who posted the previously unknown vulnerability which allows the hackers to penetrate the system would have some culpability in the compromise. It is instructive to note that those who posted the vulnerability are regarded as 'researchers' and not as having acted negligently.

Who is really to blame?

Considering the situation, it raises the question as to who is really to blame for the breaches described in the article. Clearly, the author has blamed both victims. The victim had a previously unknown vulnerability that was identified by a "researcher" and disclosed to the company. The "researchers" offered to "help" the company and the company declined their help. When the victim did not respond as the "researchers" had intended, the "researchers" then posted the exploit online. Consequently, the victim was breached by the posted vulnerability. In the article, the blame was placed at the feet of the victim, yet no culpability ascribed to the "researcher" in spite of the fact that they publicized a vulnerability which enabled another actor to exploit said vulnerability resulting in the breach. Certainly, the first suspect of the breach would be the 'researchers' themselves. Understanding the philosophical and legal aspects of cause and causation, it is difficult to envision how someone could blame the victim for the breach. The only accusation appears to be that the victim did not agree to the offer of those who identified the vulnerability to 'help them.' The victim did state that they felt they had addressed the vulnerabilities. In response to not addressing the vulnerability as the "researchers" had intended, the "researchers" posted the vulnerability resulting in the breach.

Multidimensional Failures (industry, system, law enforcement)

Recently I was sharing a taxi with a woman who was a professor at a large, well known university. She asked me about my job and I indicated I was a data security professional. She curtly responded by saying that I should say "lack of security" professional. I asked her to explain what she meant by security or lack of security. In an attempt to add credibility to what was to come next she did explain that, in addition to being a professor, she was a "retired tactical intelligence officer." She referenced a recent major data breach and then began to explain how companies that "did not use encryption were at fault". She then indicated, without prompting, that "even encryption can be easily broken." Upon hearing this, I asked her to explain what she meant by "using encryption". Did she mean encryption over a private network or encryption of data at rest? I then asked whether she felt that symmetric key encryption or asymmetric key encryption was preferable. Finally, I indicated that I was unaware of any

regulations or laws that required encryption on a private network but would like to know if any existed. This self-acknowledged professor and "retired tactical intelligence officer" then stated that she did not understand encryption technology very well, nor did she understand any of the regulations pertaining to data protection. Without any understanding of information security or the actual events that transpired, this person had made a judgment that the victim was at fault and was willing to defend that position in the face of contrary evidence.

As an industry, our inability to prevent cybercrime is frustrating to law enforcement professionals, security professionals and consumers alike. Since 2003, the payment card industry has been ravaged by increasingly large and significant data breaches involving consumer data. The natural response for anyone that is inconvenienced or feels victimized is to try to identify those they believe are responsible and place the blame at their feet. As Timmer and Normal said:

"But wherever victim precipitation is offered as an explanation, it serves to place responsibility on the victim: you cause, or help to cause, your own victimization; you deserve what you get."[xliv]

When we cannot hold the actual offender accountable, we want to blame someone for the crime. The easiest target is the large, faceless, "uncaring" corporate organization that *"…must have been able to do more to prevent themselves from being victimized".* When we find out that the company had a $100 million per year security budget, people claim that they "should have spent $125 million"…

According to a 2012 survey of 172 companies in six industries, current security measures are only preventing 69% of cyber-attacks against banks, utility companies and other 'critical assets'. To stop 95% of attacks, companies would need to spend 7 times (700%) more than they are spending today. This would increase spending from $5.3 billion ($30.8 million average) to $46.6 ($270.9 million average) for the industry. This, it is estimated, would still only prevent 95% of attacks. While not a consistent increase, it could be calculated that for every 1% increase in protection, another $9.23 million per company would need to be spent. If this is indeed accurate, it is clear that the current perspectives and strategy of cybersecurity is fatally flawed.[xlv]

According to the FBI's own website, in 2013 there were 38 indictments, convictions, or sentences imposed against cybercriminals.[xlvi] While laudable, considering the Privacy Rights Clearinghouse listed an average of 628 breaches from 2010 -2013 (3 years), the 38 cases would represent only 6% rate of indictment or conviction of those criminals[xlvii]. Estimates are that less than 2% of breaches are even identified.

After a recent breach, two lawmakers introduced legislation to address what they perceive as the issue. Reviewing the language and intent is educational to those interested in the idea of cybercrime and victim blaming. While standing in front of a retail location of one of the most recent victims of an organized data breach the Honorable Senator Menendez (D) New Jersey said:

> *"If in fact you have a company, whether it be [company name] or any other, that is not making the investment in their security process to* ***ensure that what happened to***

> ***(victim) doesn't happen,*** *"* he then said: *"then you have to question why a company would not do that."*

Comparing this statement with those made by the Honorable Senator Leahy (D) VT, who is focused upon increasing penalties for those committing cybercrimes, reveals an interesting difference in how assertively the Federal government is willing to pursue such cases. While introducing the Personal Data Privacy and Security Act 2011 (S1151 (112))[xlviii] for the 5th time since 2005, Senator Leahy said:

> *"CFAA reforms in the Personal Data Privacy and Security Act carefully balance the need for clear and meaningful punishment of computer crimes, with the equally compelling need to encourage innovation and to apply the law fairly. The bill includes several provisions that make clear that Congress does not intend for the Justice Department to pursue criminal prosecutions under the CFAA for conduct solely involving a violation of a terms of use agreement or contractual agreement."*[xlix]

Considering the bill has been proposed five times and has not yet passed, it raises questions as to the focus of prosecution. Since 2005, over 30 new states have adopted data breach notification laws with few, if any, focusing on prosecuting those who perpetrate such crimes. In fact, S1151 still applies obligations to companies who are victimized to notify affected consumers. Hacked companies would be required to notify their customers of a breach within 60 days. In the case of a hacked business that simply handles sensitive information but doesn't own it, the data's owner would be responsible for alerting customers to the incident. The type of information covered under the bill would include names, Social Security numbers and birth dates, among other things.

Data breach notification laws and those laws that solely focus upon compelling companies to "not be victimized" are oriented toward victimization prevention and not crime prevention. They are focused upon victim precipitation as opposed to structurally precipitated crimes. They are borne out of the failure of the system to prevent to deter crime. Consider the payment card industry. The credit card technology used in the United States dates to the 1950's which relies upon encoded magnetic stripes with no encryption or obfuscation of data. Merchants and other entities are compelled to accept this mechanism as it is simply not possible to compete in today's environment without accepting payment cards. Criminals have been preying upon payment card companies for years with near impunity. Law enforcement is incapable of keeping up with the volume of breaches. When a company is breached, they are first branded with a scarlet letter decrying their inability to maintain compliance. Companies are penalized by the card brands for 'noncompliance' and are required to pay huge sums to reimburse issuers and other participants for the violator's perceived 'insecurity' or inability to protect data. After the card brand penalties, companies are then faced with a litany of civil lawsuits as well as lawsuits from various state and Federal agencies all proclaiming that the company was 'guilty' of negligence or did not 'adequately' protect consumer data. While his statements related to auto theft in the 1970's were relevant, it is just as relevant to apply the same language to the current state of cybercrime.

> *"~~Car stealing~~ Cybercrime seems to be the only crime for which there is an organized victim-blaming lobby, a particular situation that developed long ago. Comprised of representatives of ~~auto-makers~~ payment card companies, insurance companies, the media, and law enforcement agencies, this lobby has castigated ~~motorist~~ data custodians and data owners' carelessness since the dawn of the ~~automobile~~ digital age."*[i]

Borrowing for Timmer and Normal once again for emphasis it is clear that:

> *"the ideology of victim precipitation blames neither the structure of society nor the individual offender for crime. Instead it blames the victim who precipitates the crime. The ideology of victim precipitation only leads to repressive criminological research and criminal justice practices that fail to prevent crime."*

The cybersecurity industry has reached a state where the criminals are no longer blamed for crimes in which information is compromised. The inability of law enforcement and the industry at large to deter aberrant criminal behavior has resulted in a situation in which the focus has changed from preventing crime to requiring the prevention of victimization.

Conclusion

Whether because of Schadenfreude or a simple lack of understanding of the origins of cause, crime victims of all types are frequently blamed for their own misfortune. Identifying the actual cause of a criminal event requires an understanding philosophical aspects of the concept, as well as legal aspects. It is certainly possible that some cybercrime victims could be found negligent in their duty to protect client data. Being found negligent in a court for creating an environment which is considered to play a proximate role in the breach is much different than being the 'cause' of the crime. Too often the actual criminal is excluded from the discussion in which blame is assigned. As can be seen with the Honorable Senator Mendoza's comments, the victim is usually the first party blamed for their own misfortune. Within the cybersecurity industry it is common to point the accusatory finger at any victim of a data breach. This is deleterious to the cybersecurity industry, as it creates an environment where companies have a disincentive to share information about their breach which could possibly be used to help other companies facing attack.

About the Author

Chris Mark an internationally recognized expert on the payment card industry data security standard (PCI-DSS) and security within the payment card industry. While working in information security for the past 14 years, Chris came to data security via the military serving, first as an enlisted Marine and then as a Navy officer. With specialties as a Marine Scout/Sniper and Reconnaissance Marine, and having seen combat in Somalia, Chris has been involved in numerous aspect of security from data, to physical, to force protection. In data security, he continues to draw on those experiences, knowing that technology, standards and protocols are only part of the pictured that the core of security is about people. On the other end of the technology is someone who's trying cause harm. The ultimate goal with security is to allocate resources the most efficient way possible to prevent that person from doing damage.

He's been on the frontlines of a variety of security battles, from conducting anti-piracy operations in the Gulf of Aden, to supporting anti-piracy operations for the maritime industry. Prior to that, he founded a qualified security assessor (QSA) firm and conducted or managed over 100 assessments, and trained over 2,800 QSAs worldwide. As the Visa Inc. CISP trainer, he was responsible for training another 10,000 people on PCI-DSS and related topics.

Chris has a BA, MBA and is currently pursuing a Doctorate (DSc) in Information Assurance. He is a CISSP, CIPP and possesses numerous technical certifications.

Chris's specialties include cyber espionage, risk management, and the human element of security. He prolifically speaks, writes and blogs on these topics, and has been published in *Secure Computing (SC Magazine), Transaction World, Secure Payments, The Counter Terrorist, Credit Union Times, PenTest magazines* and on PYMNTS.com, among others

Disclaimer

The views and opinions in this paper are the sole opinions of the author and do not reflect the views of his employer, company, or any other organization. This paper is provided for informational purposes only and should not be considered legal or business advice. Finally, this is not an academic paper so please excuse the non-APA format and any mis-references.

Endnotes

[i] http://www.merriam-webster.com/dictionary/schadenfreude

[ii] http://www.nj.com/business/index.ssf/2013/12/menendez_to_announce_safeguards_for_consumers_in_wake_of_target_data_breach.html

[iii] Karmen, Andrew (2012-05-08). Crime Victims: An Introduction to Victimology (Page 2). Cengage Learning. Kindle Edition

[iv] Timmer, D. A., Norman, William H. (1984). The Ideology of Victim Precipitation. Criminal Justice Review.

[v] http://dictionary.reference.com/browse/victim?s=ts

[vi] Karmen Ibid

[vii] Karmen Ibid

[viii] http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=4565&context=jclc

[ix] http://www.foxnews.com/us/2014/04/30/montana-teacher-1-month-rape-sentence-overturned/

[x] Fattah, E. (1967). Toward a criminological classification ofvictims. International Criminal Police Review, 209, 162–169.

[xi] Block, R. (1981). Victim–offender dynamics in violent crime. Journal of Criminal Law and Criminology, 72, 743–761.

[xii] Lerner, M. (1965). Evaluation of performance as a function of performer's reward and attractiveness. Journal of Personality
and Social Psychology, 1, 355–360.

[xiii] Timmer and Normal; Ibid

[xiv] http://www.merriam-webster.com/dictionary/opportunity

[xv] Felson, R. B. (1993) Predatory and Dispute-related Violence: A Social Interactionist Approach. In Clarke, R.V. and Felson, M. (eds) Advances in Criminological Theory. VOl. 5. New Brunswick. Transactions Publishers.

[xvi] Beebee, Helen; Hitchcock, Christopher; Menzies, Peter (2009-11-12). The Oxford Handbook of Causation (Oxford Handbooks in Philosophy) (p. 1). Oxford University Press. Kindle Edition.

[xvii] Minto, W. (2011-3-24). Logic, inductive and deductive. Kindle Edition. Retrieved from Amazon.com

[xviii] Finocchiaro, M. A. (1981, January). Fallacies and the evolution of reasoning. American Philosophical Quarterly, 18, pp. 13 - 22. Retrieved February 4th, 2014 from http://www.jstor.org/stable/20013887

[xix] Kirby, G. R., & Goodpaster, J. R. (2007). Thinking: An interdisciplinary approach to critical and creative thought. Upper Saddle River, N.J: Pearson Prentice Hall.

[xx] Minto ibid

[xxi] Kirby & Goodpaster ibid

[xxii] Bennett, B. (2012). Logically fallacious: The ultimate collection of over 300 logical fallacies. Sudbury: Ebookit.com

[xxiii] Bennett Ibid

[xxiv] Audi, R. (1995). The Cambridge dictionary of philosophy. Cambridge: Cambridge University Press.

[xxv] Finnochiaro Ibid

[xxvi] http://en.wikipedia.org/wiki/Fallacy

[xxvii] Finnochiaro ibid

[xxviii] Levi, D. S. (1987). In Defense of informal logic. Philophy and Rhetoric, 40(4), 227-247. Retrieved February 4th, 2014 from http://www.jstor.org/stable/40237520

[xxix] Bennett Ibid

[xxx] Minto Ibid

[xxxi] Pirie, M. (2007). How to win every argument: The use and abuse of logic. London: Continuum.

[xxxii] Vleet, V. J. E. (2012). Informal Logical Fallacies: A Brief Guide. Lanham: University Press of America

[xxxiii] Finocchiaro Ibid

[xxxiv] Beebee, Helen; Hitchcock, Christopher; Menzies, Peter (2009-11-12). The Oxford Handbook of Causation (Oxford Handbooks in Philosophy) (p. 111). Oxford University Press. Kindle Edition.

[xxxv] http://boards.straightdope.com/sdmb/showthread.php?t=677941

[xxxvi] Meltzoff, Julian (2010-06-01). Critical Thinking About Research: Psychology and Related Fields (Kindle Locations 659-661). American Psychological Association. Kindle Edition.

[xxxvii] http://epianalysis.wordpress.com/2012/11/19/chocolate/

[xxxviiixxxviii] http://en.wikipedia.org/wiki/Spurious_relationship

[xxxix] Meltzoff, Julian (2010-06-01). Critical Thinking About Research: Psychology and Related Fields (Kindle Location 617). American Psychological Association. Kindle Edition.
[xl] www.legaldictionary.com
[xli] Berkeley
[xlii] http://www.legalmatch.com/law-library/article/negligence.html
[xliii] http://blog.snapchat.com/post/71353347590/finding-friends-with-phone-numbers
[xliv] Timmer, Ibid
[xlv] http://www.bloomberg.com/news/2012-01-31/cybersecurity-disaster-seen-in-u-s-survey-citing-spending-gaps.html
[xlvi] http://www.justice.gov/criminal/cybercrime/press-releases/2013.html
[xlvii] https://www.privacyrights.org/data-breach/new
[xlviii] https://www.govtrack.us/congress/bills/112/s1151/text
[xlix] http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/09/prosecutors-used-this-cybercrime-law-against-aaron-swartz-now-a-senator-wants-to-strengthen-it/
[l] Karmen, Ibid